Topological Analysis of Power Grid to Identify Vulnerable Transmission Lines and Nodes

Premananda Panigrahi

Department of Electrical Engineering
National Institute of Technology,Rourkela
Rourkela-769008, Odisha, INDIA
May 2013

Topological Analysis of Power Grid to Identify Vulnerable Transmission Lines and Nodes

A thesis submitted in partial fulfillment of the
requirements for the degree of

Master of Technology

in

Control & Automation

by

Premananda Panigrahi
(Roll-211EE3340)

Under the Guidance of

Prof.Somnath Maity

Department of Electrical Engineering
National Institute of Technology,Rourkela
Rourkela-769008, Odisha, INDIA
2011-2013

Dedicated

to

my loving parents and my elder brother Satya

Declaration

I certify that

- The work contained in this thesis is original and has been done by me under the guidance of my supervisor(s).
- The work has not been submitted to any other Institute for any degree or diploma.
- I have followed the guidelines provided by the Institute in preparing the thesis.
- I have confirmed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.
- Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Further, I have taken permission from the copyright owners of the sources, whenever necessary.

Premananda Panigrahi
Rourkela, May 2013

Department of Electrical Engineering

National Institute of Technology, Rourkela

C E R T I F I C A T E

This is to certify that the thesis entitled ***"Topological Analysis of Power Grid to Identify Vulnerable Transmission Lines and Nodes"*** *by* ***Mr. Premananda Panigrahi****, submitted to the National Institute of Technology, Rourkela (Deemed University) for the award of Master of Technology by Research in* ***Electrical Engineering*** *with specialization in* ***"Control & Automation"****, is a record of bona fide research work carried out by him in the* ***Department of Electrical Engineering****, under my supervision. I believe that this thesis fulfills part of the requirements for the award of degree of Master of Technology by Research.The results embodied in the thesis have not been submitted for the award of any other degree elsewhere.*

Prof. Somnath Maity
Assistant Professor
Dept. of Electrical Engineering
National Institute of Technology
Rourkela, Odisha, 769008
INDIA

Place: N.I.T., Rourkela
Date:

Acknowledgements

First and foremost, I am truly indebted to my supervisors Professor Somnath Maity for his inspiration, excellent guidance and unwavering confidence through my study, without which this thesis would not be in its present form. I also thank them for his gracious encouragement throughout the work.

I express my gratitude to Prof. Bidyadhar Subudhi, Prof. Sandip Ghosh, Prof. Subhojit Ghosh, Prof. Susovan Samanta for their advise and care. I am also very much obliged to Head of the Department of Electrical Engineering, NIT Rourkela for providing all the possible facilities towards this work. Thanks also to other faculty members in the department.

I also express my gratitude to Prof. Biplab Ganguly from physics department for his excellent guidance and unwavering confidence through my study and also to PhD research scholars Satyabrata Satpathy at Physics Lab, Physics Dept., NIT Rourkela, for his enjoyable and helpful company I had with.

My wholehearted gratitude to my parents and my elder brother Satya for their encouragement, love, wishes and support. Above all, I thank Almighty who showered his blessings upon us.

Premananda Panigrahi

Rourkela, May 2013

Contents

List of Abbreviations

Abbreviation	Description
CNT	Complex network theory
DLA	Dynamic line attack
SLA	Static line attack
HBNLA	High betweenness node less reactance line attack
DHDN	Dynamic high degree node attack
SHDN	Static high degree node attack
RA	Random attack

List of Figures

Abstract

Electrical energy generation and distribution systems are good examples of complex systems. This M.Tech thesis is dedicated to the study of Complex Network Theory with applications in power systems for the analysis of vulnerability in power grid both for unweighted and weighted network. In Power system the vulnerability has been a key issue since a decade. A simple component failure may cause cascades of failures across the power grid and lead to a large blackout. A number of recent large blackouts in Europe, North America and India have emphasized the importance of understanding the dynamics. In this thesis Power grids have been studied for their structural vulnerabilities using purely topological approaches. The focus of the study is for a complete topological analysis of power grid based on different mode of attack. Analysis has been done by modeling power grid as a topological network and applying the concepts from graph theory. The work can be broadly classified into two parts: first is vulnerability analysis of unweighted small world network and second is analysis of weighted network in terms of homogeneous and heterogeneous network. In particular, this thesis propose two new method to identify vulnerable line for both the network and compare the topological structure of unweighted small world network with weighted network. The simulation has been done for IEEE 39, 118 and 300 bus. It is demonstrated by simulations that failure of transmission lines identified as critical, has a major impact on the performance and structure of the network unlike the failure of random connections which have no effect.

Chapter 1

INTRODUCTION

1.1 OVERVIEW

The chapter 1 gives an overall background and the purpose of this research work. Section $1 \cdot 2$ gives brief idea about the purpose of this work. Section $1 \cdot 3$ introduces fundamentals of network science along with its brief history and applications. A brief background of power system and its relation with complex network is given in Section $1 \cdot 4$ and Section $1 \cdot 5$ discusses the motivation and scope for this research study. Next in Section $1 \cdot 6$, the objectives and contributions of this research are highlighted. Finally, the chapter concludes with the structure of this thesis in Section $1 \cdot 7$.

1.2 PROLOGUE

The power system support the power generation, power transmission and distribution operations. Recent development in the field of energy transmission and distribution along with its production, increase the security of power grid by using digital technology which can save energy, reduce cost and increase reliability, and furthermore, assist reduction in greenhouse gas emissions. This modern technology is called smart grids.

Day to day increase demand in power makes the power system very crucial in our life. Like other network (Internet, Air traffic and road), power system also vulnerable to attack and failures. In some cases, a common faults can

trigger a cascading failure and eventual blackouts, which may cause huge financial loss to power utilities. In order to maintain the stability of power grid, it is essential to minimize such problems and fix them quickly if they occur. Therefore, intensive research is needed to study the robustness and vulnerability of a power network.

Since a long time Complex network theory has been studied extensively to analyze different complex network (biological systems, social networks and internet networks) due to its potential for solving large scale practical problems in a easier way. Intensive studies shows that those complex network display substantial topological features.

In 1998 watts and strogatz small world network shows that the complex structure like power grid can also studied by the help of complex network which provided a new direction to power system research. Based on graph theory a power system can be modeled as a graph with nodes and vertices and further analysis can help in identifying the critical lines and locating faults by doing the topological analysis. Current research is an effort to add knowledge to the existing techniques for structural vulnerability analysis of a power networks. The thesis is devoted to the study of vulnerability analysis under different mode of attack for both weighted and unweighted network using Complex Network Theory.

1.3 NETWORK SCIENCE

The science of Complex Network Theory (CNT) has been evolved in the 1700, but the practical application in mathematics and engineering has been done in the late 1990. In 1736, Swiss mathematician Leonhard Euler solved the problem of Konigsberg in the best way using graph theory. In 1960 and 1970, the CNT was used by researchers in different field like social science to model social networks to study the behavior of humans in groups. The famous experiment by Stanley Milgrams known as six degrees of separation [2], suggested that, if any two people selected randomly from any place in the world than they were separated from each other by approximately six (or

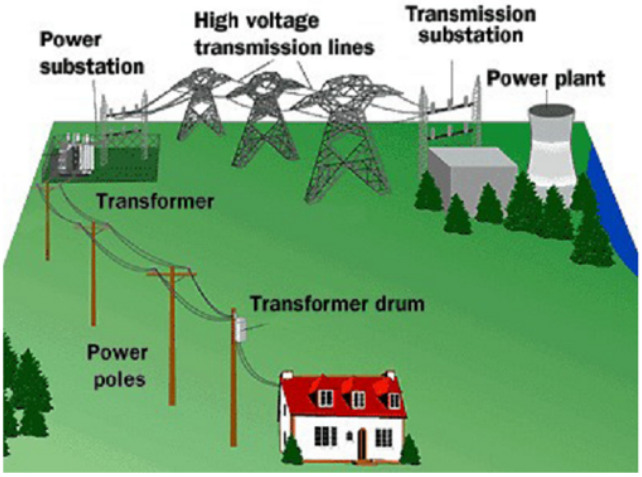

Figure 1.1: Schematic of a Simple Power System

less)intermediate connections. He introduce the idea of small world network. This type of idea boost the research field towards different complex network model. Researchers came up with different models like, regular, random, small world and scale free networks in an attempt to explain the functionality and behavior of complex real world systems [3]. The study of modern network theory includes both static as well as the dynamic properties. The static properties relate to the topology of the system and the dynamic properties explain the function or behavior.

1.4 POWER SYSTEMS

The power system is composed of power plant where electrical power is generated, transmission sub-station where electricity is transmitted to the load and high voltage transmission lines and electrical components, which are used to transmit electrical power. On a very basic level we can say power generated and transmitted to the transmission substation, where power is stepped-up to the transmission voltage level, then this power is transmitted the distribution substation where it is stepped down to distribution level to transmit over low voltage distribution lines to consumers. Figure $1 \cdot 1$ shows the schematic of a typical power system. The power generation plants like thermal plants, nuclear plants, solar, wind, hydro all have different mechanisms and control

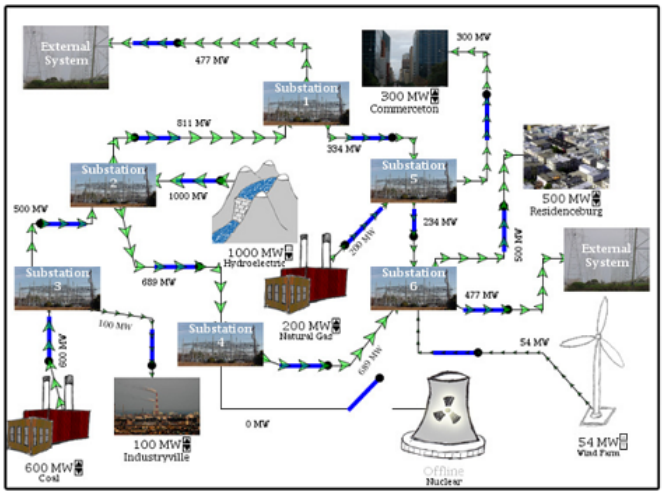

Figure 1.2: Schematic of a Power Network

strategies. These generation unit are connected with each other. Similarly, there are a variety of loads too like household consumers, offices, small-scale industries, large-scale industries etc. When all of these generation and load unit are put together, it starts to form a very complex network as shown in figure $1 \cdot 2$. The different component in power grid which forms nodes or edges have different vulnerability label depends on the function and location in the network. Some times failure of some of them can have a large impact on the whole power system while failure of others might have small or no effect. So safety and reliability can be achieved by the proper maintenance of each element and monitor them accordingly.

Power System as a Complex Network

A power grid can be modeled as complex network. The generators, bus bars, transmission bars and loads bars are modeled as nodes and the connecting transmission lines are modeled as edges. The power grid is considered to be a small world network [4], some of the power grid are small world network with characteristics of scale free network [4] [5] [6].

Network	Description
Internet	Internet is a very huge network having physical connections between computer and n-numbers of other communication devices. In graph theoretical studies the routers are the nodes and the physical connections between them are edges.
World Wide Web	World Wide Web represents one of the largest network among all other network, for which the topological information is not known. The web pages are the nodes and the hyperlinks which point to these pages are the edges. They are an example of scale free network.
Movie actor collaboration network	This type of network comes under small world network, 6 degree separation concept is well fitted with this. In this network, the actors are the nodes edges are the relation between two actors.
Science collaboration network	This network is similar to the movie actor network except that here the nodes are researchers and they have a connection between them if they have publish a paper together.
Cellular networks	This is a biological network and in this network, different substrates are the nodes and directed chemical reactions in which these substrates participate form the edges.
The web of human contacts	This type of network studies the human relationships. The human beings are the nodes in such networks. If one human know other human except from his family member then there is an edge between two nodes, if they communicate or socialize in any way. NGO organization is one of the example.
Power networks	A power grid is an example of small world network. Power grid from USA, china shows the behavior of small world network. Also some power grid are small world network but showing the behavior of scale free network. In these networks, generators, bus bars, loads, transformer, substations etc can be modelled as nodes and the transmission lines connecting them are considered to be edges. Current study relates to the modelling, vulnerability analysis and fault location in power systems using Complex network theory.

1.5 MOTIVATION AND SCOPE

1.5.1 Motivation

From 1970 the Complex Network Theory has significant applications in social, biological and internet networks and now slowly it is making its way for the topological analysis of power system. More and more researchers applying this complex theory for modeling and analysis of power grid. Day by day new research is going on and better models are emerging with advancement in power system research, it is still now at an early stage and there is a lot of scope for improvement in different complex model to power grid. There need to be more improvement in complex network model when its characteristics are applied to the real power grid. So as to enable researchers to do a more accurate structural vulnerability and reliability assessment

Researchers have come up with various models like Random, small world and scale free, to analyze the vulnerability and explain the propagation of cascading failures. Identification of vulnerable component with in network is not so easy, for which accuracy and perfection is needed, otherwise one simple mistake will cost much more. The failure of these components has a larger impact on the performance of the whole system. If they can be identified then the overall system security and reliability can be increased by proper maintenance and monitoring them.

In power system both power transmission lines and nodes plays a crucial role for triggering a cascading failure. The transmission lines can experience faults due to electrical or physical breakdown or over load condition which could cause interruption to reliable power supply also few of these lines are more important than others either due to their geographical structure in the network or due to the load they carry. If these important lines fail then the efficiency of the whole system can drop significantly. If a generating node or transmitting node failed than there is a possibilities of islanding. Hence this research is motivated by identification of such critical and vulnerable

lines as well as important nodes using few concepts from CNT. This part of the study also assesses the cascading failures in power systems using some existing models for such failures and compare the result of both weighted and unweighted network. So, part of this research work is dedicated to different mode of attack by studying the network topology and using concepts from network theory to understand the vulnerability of power grid.

1.5.2 Research Scope

The first part of this thesis is dedicated to identification of vulnerable lines and nodes in terms of different mode of attack. A power system is modeled as a network, where generators, bus bars, loads, substations are modeled as nodes and transmission lines are modeled as the edges. But in power system it is very difficult to consider all the electrical and topological properties at the same time. Hence, the network is modeled using connection sparse matrix. In first part of this thesis weights of each transmission line are declared 1 that means all the weight value are identical but in second part of the work weight are taken as the reactance of each power transmission line.All the methodologies and analysis are demonstrated and validated by MATLAB programming, Gephi and cytosacpe.

1.6 THESIS OBJECTIVES AND CONTRIBUTIONS

1.6.1 Objectives

The overall goals of this work can be broadly classified in to two parts

- Vulnerability analysis of power systems.
- Comparing comparison between heterogeneous and homogeneous power grid network.

Goals

- To identify the vulnerable lines and nodes which may cause blackout of any power network using concepts from Complex network model.
- To assess the cascading failures in power systems using network theory.

- To investigate the performance of the network under several mode of attack.

1.6.2 Contributions

The Contribution of this research are given below:

- In this work several mode of attack has been performed, in which two new intentional line attack mode are proposed and it gives good result comparison to other attack.
- For a small world network both weighted and unweighted network are compared after analyzing the result.
- A comparison between heterogeneous and homogeneous network has been done.

1.7 STRUCTURE OF THESIS

This thesis is structured into 5 chapter

Chapter 1 gives brief idea about the problem of this research. It gives some basic idea about complex network and the various models which exist. Next, a power system is introduced as a complex network. Further, it outlines the scope and motivation of this research. At the end of this chapter the research objectives and contributions of this study are highlighted.

Chapter 2 presents a complete literature review of the research undertaken. It starts with basic concepts of Complex network theory. Next, it discusses about the different complex model and how it is related to real time complex network, like internet, road etc etc. Further, it explains the relation of power system network with small world network and the vulnerability and cascading failures in power systems, followed by a comprehensive literature survey of work done by other researchers. Final part of the chapter discusses the various fault location techniques in power systems and a literature survey of the work done in the past.

Chapter 3 presents the vulnerability assessment of power networks using

the shortest path betweenness approach. A new betweenness index is proposed using the reactance of transmission line as the matrix weight based on the power flow model for a lossless line. It has been shown that if the lines identified as vulnerable are disconnected then the efficiency of the network drops significantly unlike random failures which have less effect.

Chapter 4 presents another novel approach to analyze the vulnerability of power networks. In this study, a power network is modelled using the admittance of the transmission line as the matrix weight. Further, the maximum flow based centrality approach is used to index the lines based on the portion of power flow they carry through the network. It is shown that some of the lines carry significantly higher portion of flow as compared to others and they are classified as important and vulnerable. It is demonstrated that the removal of lines identified as critical have a much higher impact on the performance of the network as compared to random line disconnections. It is also shown that the failure of random lines cause little load shift to adjacent lines whereas, the outage of critical lines have a huge load shift throughout the network which could potentially lead to cascading failures.

Chapter 5 presents conclusion and future scope of this work.

1.8 SUMMARY

This chapter has introduced complex systems and discussed the various existing models. It has also described a power system and discussed some of the problems which need attention and how they can be addressed using Complex Network Theory. Further, it has briefly highlighted the motivations and scope of this research and listed the main contributions. Finally, the thesis structure and main contents of each chapter is briefly outlined towards the end.

Chapter 2

LITERATURE REVIEW

2.1 OVERVIEW

This chapter gives a complete literature survey of the existing technologies and work done for the identification of vulnerable component by other researchers until now. It mainly covers fundamentals of complex systems, vulnerability analysis of power systems. Section $2 \cdot 1$ starts with some basic concepts of complex networks and measurement parameters based on the work done here. Next, in Section $2 \cdot 3$ a power system is introduced along with techniques to modeling it in terms of topological model. Section $2 \cdot 4$ discusses the vulnerabilities of complex systems. Reviews all existing works relating to power systems vulnerability and cascading failures are done in Section $2 \cdot 5$. Finally, Section $2 \cdot 6$ gives idea about the software's used in this research.

2.2 COMPLEX NETWORK THEORY

A network can be defined by its structure (connection of nodes and links) and behavior which is a result of interaction between these nodes and links. We can say that networks are representation or models of real world systems and their behavior but not the systems themselves. It can be summarized that Complex Network Theory is the study of structure and dynamical function of a collection of nodes and links that represent something real [1].

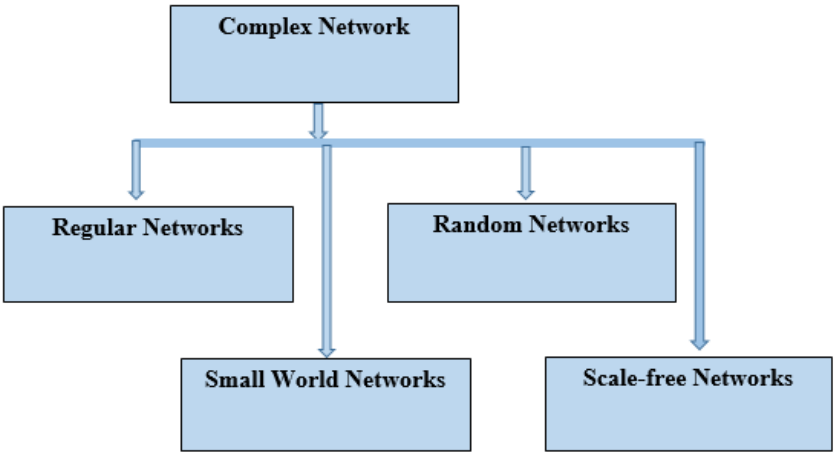

Figure 2.1: Types of Complex Networks

The topology structure of a network can be easily modeled using the graph theory. When a network modeled by using graph theory it can be defined as a set, $G=\{N,L,W\}$ where N is the set of nodes, L is the set of links and W is the weight of links. Most of the complex real systems in the world can be modeled and analyzed in the form of a complex network. To study the topological characteristics and behavior of such complex system several network models have been proposed. In the figure below, the types of networks can be broadly classified as regular, small world, random and scale-free [8] [9] [10] [11]. Figure $2 \cdot 2$ shows a simple rewiring diagram which illustrates the relationship between regular, random and small world networks [7]. The regular network starts with a ring lattice with n=20 nodes and each of them connected to four of their neighbors. Let each edge be rewired randomly with a probability P i.e. P is the ratio of number of lines rewired randomly versus total number of lines. Then, for $P = 0$, the original lattice is unchanged and i.e become the regular network. As the value of P is increased up to $P = 1$, where all the lines are rewired randomly. The small world network present in between regular and random network i.e. $0<p<1$. These three model are differentiated from each other in terms of their average path length and clustering coefficient. Which are described below.

Regular Network: In the past complex network researchers assume that,

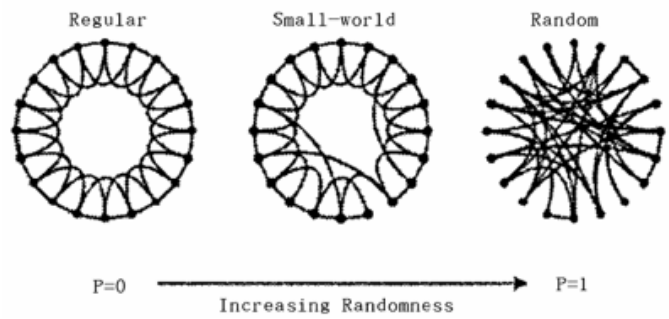

Figure 2.2: Relationship between Network Models and Randomness

most of the real network topology can be fitted with regular network, but regular net model is not sufficient to describe the networks behavior in the real world. With large average path length and highly clustered coefficient the regular model $P = 0$ forms a simple architecture, which allows us to focus on the complexity caused by the non-linear dynamics of nodes and edges without the additional complexity of the topology itself. This type of network are used to study dynamical systems such as disease spread, ecosystems etc.

Random Network: Failure of regular network to define the characteristics of most of the real network draw the attention of the researchers to develop a new model which can explain most of the important characteristics of real world network like power grid, internet, telecom etc. In 1959, Erdos and Renyi put forward the concept of random network that greatly promoted the network research [12]. The concept random means, each node within a network randomly connected with each other with a probability P=1 for which the average path length become small and small clustering coefficient [13]. The random network model fits with some of the real networks well, but this model also not able to explain some important characteristics, emerging in the dynamic evolution system with it. This type of models are more robust to intentional attack and fragile to random attack [14].

Small World Networks: It is not surprising to see that the regular lattice model and the random model both fail to reproduce some important features of many real networks. It was found that most of these real-world networks

are neither entirely regular nor entirely random. The reality is that people usually know their neighbors, but their circumstances may not be confined to those who live right next door. On the other hand, cases like links among Web pages on the WWW were certainly not created at random, as the Erdos and Renyi process would expect. With an idea to describe a transition from a regular lattice to a random graph, in 1998 Watts and Strogatz proposed the Small World network model which is a breakthrough in the research of complex network [7] [13] [15]. A small-world network is a type of graph in which most nodes are not neighbors of one another but most of these nodes among the network can be reached from every other by a small number. Small world does not mean that world is small, it signifies that the relation between people become more closer, this concept was taken from famous experiment of Milliman's which says that friend of a friend is also a friend. Specifically, a small-world network is defined to be a network where the typical distance between two randomly chosen nodes grows proportionally to the logarithm of the number of nodes N in the network [7]. The behavior of small world network falls in-between regular and random network model. In the figure $2 \cdot 2$, we can see that when the probability of connection between two node P=0, a regular network is formed and when the probability P=1 it forms random network but for a non-zero but P<1, the result will be a small-world network. The small world network is the result of rewiring procedure. Rewiring means shifting one end of the connection to a new node chosen at random from the whole network by keeping fix one end of the connection, with the constraints that any two different nodes cannot have parallel connection between them, and no self-connection node should be present in a network. It the above figure we can see that, rewiring for a small probability, the average path length drops rapidly in the same order as the one for random networks $L(p)>>L(0)$ at the same time the local properties of the network is nearly the same as those for the original regular network, and clustering coefficient does not differ from its initial value $C(p)\sim C(0)$ According to Watts and Stro-

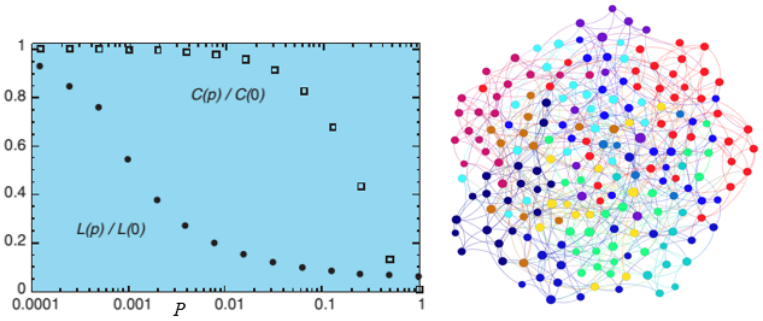

Figure 2.3: Average path length and clustering coefficient of the WS small-world model as a function of the rewiring probability

gatz, there is always a shortcut link present in most of the real network and most of the information is passed through this shortcut link, which make it more important link in between other link present within the network. This means in a small world network, the shortest path length between two nodes is likely to be relatively small and the clustering will be high [16]. US power grid is one of the example of small world network.

Scale Free Networks: In 1999 Barabasi and Albert (BA) [16]found a common feature between ER random graph and the WS small-world models is that the node distribution of the network is homogenous, with peak at an average value and decay exponentially. Such networks are called exponential networks. They discover that in the field of complex networks that a number of large-scale complex networks, including the WWW, metabolic, and internet networks, are scale-free and their node connectivity distributions have a power-law form where most nodes have low node connectivity but some of them are highly connected to the other nodes in the network [17]. This makes those highly connected nodes very vulnerable to intentional attacks and robust to random attack [14]. To explain the power-law degree distribution, Barabasi and Albert (BA) proposed another new network model called scale-free network model.

2.2.1 Preliminaries

A topological network can be defined as a set of nodes with connection edges. A vertex or node are connected together by lines called edges, or a tie. The

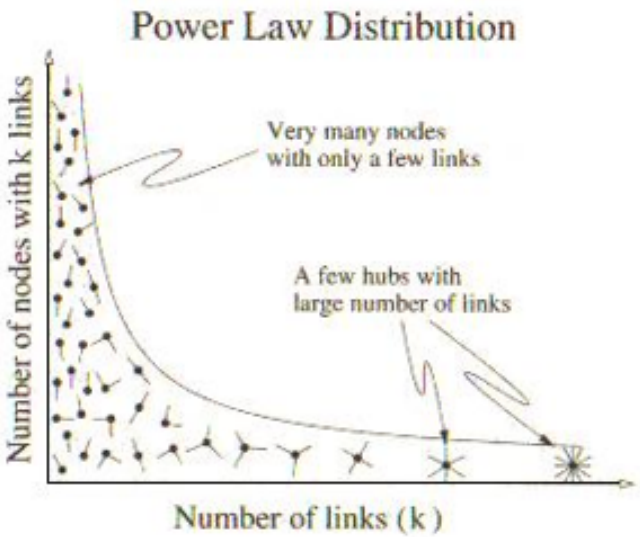

Figure 2.4: power law degree distribution between nodes and link

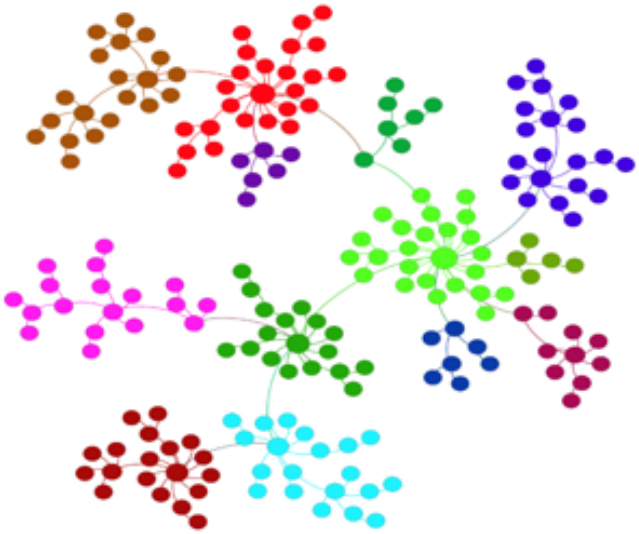

Figure 2.5: Scale free network

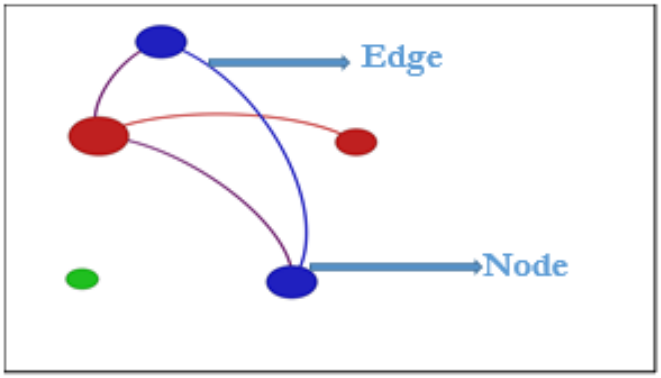

Figure 2.6: A simple graph

nodes or vertex is the representation of various elements like people, hardware devices, disease etc, and the edges represent the relationship between these nodes. Figure $2 \cdot 8$ shows a simple network with 5 nodes and 4 edges. Networks can be of different types like, networks with similar nodes and edges or may be a networks with more than similar kind of nodes and different type of edges. Network also differentiated according to their properties like in a network all the edges have same weight 1, which are called unweighted network. Some cases the edges can have weights associated with them which might represent how strongly or loosely any two nodes are connected. Such type of networks are called weighted networks. For example in a electric power grid weight is impedance. Sometimes, the flow of information can be only in one direction in which case, the network is termed as directed graphs or digraphs. The network showing properties of small world network are considered to be undirected networks in which flow of information can be in both directions of connections.

2.2.2 Survey of Measurement, unweighted

Connectivity related measurement

Degree: For a undirected network G the degree of a node is defined as the number of edges connected to a node. For example in the figure $2 \cdot 10$ the degree of node 1 is 3, as three edges are connected to it. Mathematically it

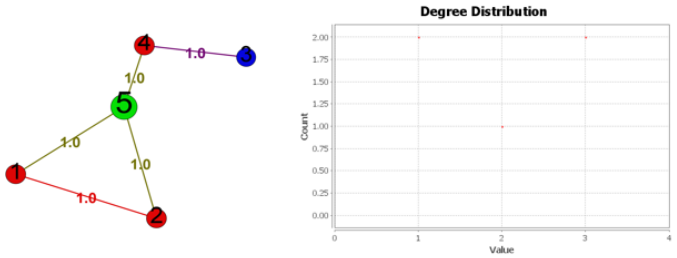

Figure 2.7: Example of Network Connectivity (a) Degree (b) Degree Distribution (unweighted)

can be written as

$$d_v = \sum_{l \in L} \delta_l^v \tag{2.1}$$

where

$$\delta_l^v = \begin{cases} 1, & edge\ l\ is\ adjacent\ to\ node\ v \\ 0, & otherwise \end{cases} \tag{2.2}$$

In a network there is a chances of a node having a particular degree is represented by a node probability distribution, also it is abbreviated as degree distribution. In fig $2 \cdot 9$ we can see the graph where node of same degree are differentiated from each other. In a weighted network, the degree dv of node v the sum of the weights of all the edges that are adjacent to v. The figure $2 \cdot 10$ (a) shows a simple weighted network where each edge has different weight value, (b) shows its degree distribution. **Clustering coefficient:** The clustering coefficient C is the measure of the average closeness between nodes in graph G or we can say the clustering coefficient measures the degree to which the nodes in a network tends to cluster together. Average clustering coefficient can be given as

$$C = \frac{1}{N} \sum_{i \in G} C_i \tag{2.3}$$

Where N is the number of node in a network G, i is the node in the network G , C is the clustering coefficient, N is the number of nodes in the network, and C_i is the ratio of actual number of links from node i to its neighboring nodes.

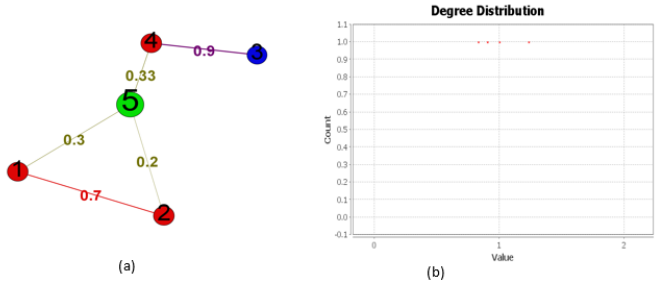

Figure 2.8: Example of Network Connectivity (a) Degree (b) Degree Distribution (weighted)

Distance related measurements

Path: When there is no repetition of vertex or edges during traveling from one node to another node is called path. In case of a undirected unweighted network, the number of edges between two node is called path length.

Average path length: In a small world network the most important quantities to characterize the properties of a graph is the geodesic distance, or the shortest path length between two vertices (popularly known in social networks as "six degree separation" or degrees of separation [2]). It was assumed that, in a small world network information always takes the shortest path to flow between a pair of node. The shortest path length d_{ij} between node i and j is the minimum number of edges traversed between vertex i to another vertex j. By taking the average of shortest distance between two nodes over the entire network is called as average path length or **characteristics path length *L***

$$L = \frac{1}{N(N-1)} \sum_{i \neq j}^{N} d_{ij} \tag{2.4}$$

The longest geodesic path between the nodes in a network is termed as diameter. In case of a weighted network the shortest path calculation is completely different from unweighted network. In fig 2.12(a) a simple example of a weighted network is given. The shortest path in a weighted complex network is the minimum of sum of total weight between two nodes. In the

above example the shortest path between node 1 and node 2 is

$$\begin{aligned} W_{12} &= \min\{w_{15}+w_{52}, w_{12}\} \\ W_{12} &= 0.5 \end{aligned} \tag{2.5}$$

Centrality measurements: In a complex network there are few such vertex and edges present, which play a important role among all other vertex and edges within it. So to find these important component some parameters of complex network are used, like betweenness centrality for both edge and node and degree of a node. The betweenness centrality is define as the number of times a geodesic path passed through a node or edge.
Betweenness centrality of edge can be written as mathematically:

$$B(l) = \sum_{i,j} \frac{\sigma_{ij}(l)}{\sigma_{ij}} \tag{2.6}$$

Where $\sigma_{ij}(l)$ is the number of shortest path passed through the edge l and σ_{ij} is the total number of shortest path from node i to node j. The sum is taken over all distinct pair of nodes i and j. Highest the betweenness centrality makes the edge more vulnerable.
Betweenness centrality of a node is define as

$$B(v) = \sum_{i,j} \frac{\sigma_{ij}(v)}{\sigma_{ij}} \tag{2.7}$$

Where $\sigma_{ij}(v)$ is the number of shortest path passed through the vertex v and σ_{ij} is the total number of shortest path from node i to node j. Highest the betweenness centrality makes the node more vulnerable than other node.

2.2.3 Search Algorithms [1]

Based on same properties of complex network search algorithms are used to find an item from a set of other items. In our work, the search algorithms is used to find nodes or edges which satisfy certain properties of complex network; let's take an example, to find the shortest path length between any source node to destination node within a network we need an algorithm. The network search algorithms can be classified as Depth First Search, Breadth

First Search, Dijkstra's algorithm and Floyd-Warshall algorithm etc. In our work we have followed Dijkstra's and Floyd-Warshall algorithm.

2.3 MODELING POWER SYSTEM AS UNDIRECTED GRAPHS

A power system is a complex network can be modeled as a graph by considering the generator, transmission and load bus as nodes and the high voltage transmission line as edges. Mathematically it can be written as *G= (N, L, W)*, where G is the network, L is the set of edges, N is the set of node and W is the set of weight. To model a power grid using CNT connection matrix E is used, where E= e_{ij}, it is also known as adjacency matrix. In figure $2 \cdot 11$ (a) 5 nodes and 5 edges are present. If there is a connection present between two node than $e_{ij} = 1$ otherwise $e_{ij} = 0$. The connection matrix

$$E = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

For a weighted network, weights can be added to each transmission line which could be a measure of electrical or topological property depending on the application. In that case, the weight value 1's will be replaced by the weights taken for that link. In case of a power grid reactance is taken as weight of link.

2.4 VULNERABILITY OF COMPLEX NETWORKS

2.4.1 Vulnerability and Robustness

The literal meaning of vulnerability means affected part, definitely in a power grid an affected part leans to component failure which may cause cascading failure and cascading failure can trigger a large blackout. So vulnerability put a large impact on the performance of the system or we can say it is a measure of performance degradation when a component in a complex network

or a power grid in our project is attacked. But robustness can be treated as exact opposite to vulnerability. It shows the capability to sustain to any type of attack in a network. It means that the system will withstand in its position based on its structure and functionality or we can say the system will regain after being exposed to disturbances.

In network structures, there are some nodes and links present which play a crucial role than all other nodes and edges. It is important to find out those important component. Some researchers in their work relate the vulnerability or robustness of networks to their connectivity [18]. Nodes with higher degree are found critical also centrality indexes are used to assess the vulnerability of a network.

Efficiency of a network The attack on links or vertices with a higher betweenness centrality index causes a bigger impact on the performance of the network which is termed as efficiency of a complex network. Latora and Marchiori proposed that Global efficiency [13], is the measure of performance of the network, under the assumption that the efficiency for sending information between two nodes i and j is proportional to the reciprocal of their minimum distance.

$$\eta = \frac{1}{N(N-1)} \sum_{i \neq j}^{N} \frac{1}{d_{ij}} \tag{2.8}$$

So, some references [19] [20]relate vulnerability to the decrease in efficiency of the system when certain nodes or edges fail or are attacked.

Giant component The giant component is one of the important complex parameter used to measure the damage caused by a cascade in terms of the relative size S of the largest connected component

$$S = \frac{N\prime}{N} \tag{2.9}$$

Where $N\prime$ and are the numbers of nodes in the largest connected component after and before the attack.

2.4.2 Methods to Assess Vulnerability of Nodes and Edges

In a complex network model to assess the vulnerability, certain nodes or edges should be removed [20]. To do this the, edges and nodes need to be ranked based on some mathematical analysis. Usually, in CNT, statistical measures such as betweenness centrality or degree are used to decide the criticality of a link or vertex [9]. Degree is the measure of number of edges connected to any node, and the higher the degree more important is that node. Motter and lai worked on load based node, where they considered the load at a node is then the total number of shortest paths passing through the node [21]. However betweenness centrality of node closely related to their concept. The edge or node with higher centrality index is ranked as more critical [8] [9] [11]. The importance of these element can be assess by removing the node or edges in different attacking mode. In our work we have considered 8 different attacking mode for both line and node attack.

Network failure and different attack modes

In this paper two attack modes based on node degree and betweenness with distinct features are considered, which include the random attack mode and the intentional attack mode. Intentional attack is more destructive than random attack, small world network shows a robust behavior to random attack, and more fragile to intentional attack [21]. We classify the intentional attack modes into different subcategories. **Line base attack:**

- Line betweenness dynamic Attack- Intentionally attack the line with largest line betweenness, than run the algorithm to find the next line with high betweenness and attack that line.
- Line betweenness static attack-Run the algorithm and sort high betweenness line according to the ordering of the betweenness then attack one by one.

- Random attack- Attack a line in the network by choosing randomly and then gradually attack more lines randomly.
- High betweenness node less reactance line attack-Find the node with largest betweenness, than intentionally attack the line with less reactance connected to that node, again run the algorithm and follow same process.

Node base attack:

- Node betweenness attack: Calculate the high betweenness node and attack the node with the largest node betweenness and then attack the nodes according to the ordering of their betweenness.
- Node degree static attack- Attack the node with the highest node degree and then attack the nodes according to the ordering of their node degrees in decreasing order.
- Node degree dynamic attack: Attack the node with the largest node degree, than again recalculate the nodes degrees and then repeat the attacking on the node having highest node degree and calculation process after each attack.
- Random node attack: Select any node randomly and attack that node then gradually attack more nodes randomly.

In order to assess the importance of these network elements, they are removed in accordance with the attacking mode given above based on degree or centrality. After calculating the value of degree and centrality for nodes and edges the network efficiency and giant component can be calculated after every attack [22]. However, as more and more nodes and edges are attack removed, the network structure changes and the network will behave differently under different strategies.

2.5 VULNERABILITY OF POWER NETWORKS

Security and operation of power system being always an important issue for power supply. So these things needs to be carefully analyzed and evaluated in order maintain the reliability and performance of the network [23]. The power system is one of the most critical complex network. However, like any other network, there are certain nodes and links present in power systems which are critical due to their function, geographical position or may be due to transmission capacity of lines or nodes and can make the system very vulnerable to intentional attacks. So their identification and proper maintenance can reduce the effort and time for monitoring such a complex systems.

2.5.1 Cascading Failures in Power Networks

Power grid structure is a growing network, everyday there will be a continuous growth in size and complexity, which brings new challenges to engineers in the field of power generation and its transmission to load distribution [24]. Disturbance in any system may trigger a cascading failure. Broadly we can say if there is a fault in one element, then it may trigger a failure of successive elements and eventually the whole network will collapses, this procedure of failure is called cascading failure. A cascading of failure may leading to blackout, when failures continue at some critical location or element due to overload condition or may be some other reason. Overload condition is one of the measure phenomenon for series failure. For instance, if a line carrying power failed due to some attack or some other reason, than the total power will be shifted to its adjacent line or node and this might cause a few of those adjacent lines to overload and fail and again load will shifted. If this process is continue without any intervention then it will lead to a complete system collapse.

Now a days another measure problem that is network hacking and intentional attacks is shown in the security of power system. There are some

Articles	Location	Day	Millions Affected
July 2012 India blackout	India	30 and 31 July 2012	620
2005 Java–Bali blackout	Indonesia	18 Aug 2005	100
1999 Southern Brazil blackout	Brazil	11 March 1999	97
2009 Brazil and Paraguay blackout	Brazil, Paraguay	10–11 Nov 2009	87
Northeast blackout of 2003	United States, Canada	14–15 Aug 2003	55
2003 Italy blackout	Italy, Switzerland, Austria, Slovenia, Croatia	28 Sep 2003	55

Figure 2.9: Famous and largest black out

critical links and nodes present in power grid, which make the system very vulnerable to terrorist attacks. If a terrorist has the knowledge about a power grid, then he can target the most vulnerable elements which may lead to a cascading failure. Hence it is important to do a vulnerability analysis and to identify those critical parts of the network and monitor them. Figure 2.13 shows the satellite image of one of the largest blackout of Northeastern United States which happens in 2003. In these two images, the images on left is before the blackout and the one on right is after the blackout where most part of the city is plunged in darkness.

2.5.2 A Survey on Research Paper

- Albert et al. [23] study the United States Power Grid and its reliability under attack. They build a graph consisting of 14099 nodes and 19657 edges, based on the information of the POWER map system

- Motter and Lai [21] have differentiated between heterogeneous and homogeneous network structure. Heterogeneous structure are more vulnerable than homogeneous network for intentional attacks, He shows when a link is attacked its load can be redistributed among nodes can lead to cascade of overload failures, which may cause the entire system to collapse.

- Zongxiang et al. [25] have shown that most of the power systems like in USA China, are usually comes under small-world network structure and then he used the collective dynamics of those network models to analyze cascading failures.

- Albert et al studied the structural vulnerability of the North American power grid [26].

- The large-scale blackouts motivated Crucitti et al. [6] to analyze the cascading failure in the Italian power grid [27].

- Casals et al. [28]analyzed the European Power Grid and its topological structure. He try to extract the non-topological reliability measures by analyzing topological properties of the network and its tolerance to failures and attacks.

- Sole et al. [29]have worked on the same power grid and explored the fragility of the European power grid under intentional or terrorist attacks.

- Watts [15] explore the properties of the U.S Power Grid. He treated this Grid as an undirected unweighted graph in which all the nodes of the network are equally considered as nodes and all the high voltage transmission line are considered as unweighted edges. The graph has 4941 nodes, which is quite large.

- Mei et al. [30]did various simulation related to Power Grid vulnerability and blackout conditions considering IEEE synthetic model like IEEE 14,

30, 39 and 118-bus and also simulate the real Chinese Power Grid by taking its sample.

- Pepyne [31]studied and evaluate the cascading effects of IEEE model (IEEE 57-Bus and IEEE 118-Bus) and on a sample with of 200 nodes and 400 edges, satisfying the small-world model [1].
- Chen et al. studied the power grid based on small world network and use CNT parameter like betweenness and efficiency based on shortest path to identify the critical lines in power networks.

2.6 SUMMARY

This chapter present a thorough survey of literature in complex network theory and its relation with power systems, particularly related to vulnerability assessment of power grid. This chapter discussed the overall application of Complex Network Theory in vulnerability analysis along with the concepts which have been used throughout this research. Also different intentional attacking mode with two new proposed attacking mode are discussed. Overall, this chapter serves as a foundation for the rest of the thesis.

Chapter 3

ANALYSIS OF UNWEIGHTED NETWORK

3.1 OVERVIEW

This chapter discusses the vulnerability assessment of synthetic grid from IEEE literature (IEEE 39, 118, 300 bus) using the betweenness centrality and degree of node approach. In section $3 \cdot 2$ some preliminaries relevant to this study are given. Section $3 \cdot 3$ gives the idea about the vulnerability analysis of IEEE networks using the shortest path betweenness and nodal degree analyze by which mode of attack the grid is affected much more in terms of performance of the network and decrease in giant component size. Based on two properties of complex network, one is betweenness of edge and node and another is degree of node, removal of edges and nodes in IEEE synthetic network are performed. After each attack to the line or node, efficiency and giant component size are measured. Attacking method that we have followed are given below [20]:

Line Base Attack:

- Line betweenness dynamic Attack- Intentionally attack the line with largest line betweenness, than run the algorithm to find the next line with high betweenness and attack that line.

- Line betweenness static attack-Run the algorithm and sort high betweenness line according to the ordering of the betweenness then attack one by one.
- Random attack- Attack a line in the network by choosing randomly and then gradually attack more lines randomly.
- High betweenness node less reactance line attack-Find the node with largest betweenness, than intentionally attack the line with less weightage value connected to that node, again run the algorithm and follow same process. Concept is followed from moter and lai paper. The load at a node is the total number of shortest paths passed through the node, more number of shortest path passed through a node, is highly loaded. Now from this concept we proposed that from a highly loaded node the less reactance line in a power grid is more vulnerable than all other line connected to it. As power flow is more through a less reactance path. The result was compared with other several attacking mode result for a unweighted and undirected power grid model.

Node Base Attack:

- Node betweenness attack: Calculate the high betweenness node and attack the node with the largest node betweenness and then attack the nodes according to the ordering of their betweenness.
- Node degree static attack- Attack the node with the highest node degree and then attack the nodes according to the ordering of their node degrees in decreasing order.
- Node degree dynamic attack: Attack the node with the largest node degree, than again recalculate the nodes degrees and then repeat the attacking on the node having highest node degree and calculation process after each attack.

- Random node attack: Select any node randomly and attack that node then gradually attack more nodes randomly.

3.2 SHORTEST PATH BETWEENNESS APPROACH

In our research work we have considered the power grid as small world network, some power grid like in USA, china shows the behavior of small world network. In a small world the network are assumed to be undirected and unweighted that means the weight of each line is considered to be 1 rather than real weight. During the first phase of work we have not taken into account any of the electrical properties of the real power system. Further, so many difficulty can be face during model the dynamics going on within the node of power grid. But in case of transmission line it is much simple to take into account the static properties of line. Most of the researchers found that the transmission line are exposed to more risks than nodes. Hence, we gave more emphasis to find out the vulnerable transmission line than node in our work also different attacking methodologies are proposed to identify most vulnerable links.

The information being transmitted between a transmission lines from source node to destination node is electrical power. The number of times a link is being used or in other way we can say the number of time a shortest path passed through a line in order to transfer power between source and destination node is termed as the line betweenness. Same concept is used for node betweenness. Moter and lai termed this concept as load on node. If this highly loaded node or link is removed, the average path length of the network could increase significantly leading to a drop in the efficiency as well as in giant component size of the system. Thus, this betweenness index under several attack mode could be used to identify the critical links of the network under consideration.

3.2.1 Line and Node Betweenness Calculation

The process of calculating line and node betweenness is given below

- First, calculate the shortest path from a source node i to all other nodes
- Then, starting from the node which is farthest we work towards the source node. In the process of traveling from the farthest node to source node we assign an index to each edge as well as to each node. This index is calculated as the sum of indices of all the edges and nodes leading to it plus 1
- When all the nodes in the path have been covered, the index of each edge and node gives the betweenness count for the paths and the path passed through the node from node i
- Repeat steps with different source nodes until all the nodes are covered.
- The sum of indices for all possible iterations gives the complete betweenness count for shortest paths between each pair of nodes.

3.2.2 Efficiency and Giant component of a Power Network

Until now, we haves studied that shortest path is the most convenient way for transmitting any information between two node through the network. In case of a power network most of the cases power is transmitted through the shortest path based on geographical position to minimize the cost. In Chapter 2 already we have discussed in details about efficiency and giant component of a network. Efficiency for any network is the inverse of characteristic path length [32] [27] [13]. Let's take an example of a road traffic, if due to some reason road is blocked, than people will take an alternate route which could be longer and more time consuming, in such case we can say performance of road between sources to destination is decrease. Similarly in case of power grid if we delete the most important node, i.e the short cut link, than power will redistribute through available path, in such cases performance of complete network decreases. In case of unweighted network we have consider the weight of each transmission line as 1 only to model the power grid in terms of small world network. But practically other parameter of real transmission line

need to be consider. We have consider reactance as a parameter to flow the power, which will discuss in weighted network. A thorough analysis between unweighted and weighted network will be done at end of this chapter. The giant component is one of the important complex parameter used to measure the damage caused by a cascade in terms of the relative size S of the largest connected component.

3.2.3 Identification and Assessment of Vulnerable Lines

Procedure to identify the vulnerable line

- First model the IEEE synthetic grid according to the principles mentioned in the sections $2 \cdot 3$ and generate a connection adjacency matrix E.
- Add weight value 1 to each transmission line in the network.
- Calculate the shortest electrical path matrix for a unweighted undirected network based on the adjacency matrix E.
- Calculate the line and node betweenness based on the 8 different attacking mode both for line and node.
- Mark the high betweenness line and node as more vulnerable for each different mode of attack.
- Delete the lines and nodes identified as vulnerable in order of their importance and calculate the efficiency as well as giant component size of the network using Equation $2 \cdot 8$ and $2 \cdot 9$ after every attack.

3.3 CASE STUDIES

This section describes the application of methodology explained in Section $3 \cdot 4$. The case of IEEE 39 bus system, IEEE 118 bus system and IEEE 300 bus system are undertaken and the techniques defined in previous sections are used to identify the vulnerable lines. The results are verified by the proposed attack strategies and sensitivity analysis.

3.3.1 IEEE 39 Bus System

Figure $3 \cdot 1$ shows the IEEE 39 bus system, the horizontal bold bars represent the bus bars which are considered as the nodes of the system. There are 10 generator bus bar i.e nodes, the ones with arrows are load nodes and others are transmitting nodes. The transmission lines connecting different bus bars are considered as edges. The topological structure of IEEE 39 bus system is given in fig $3 \cdot 2$, which is generated by gephi $0 \cdot 8 \cdot 2$. Node distribution shows, how a similar kind of node connected in a network. To do the topological analysis firstly, the IEEE 39 bus system shown in Fig-$3 \cdot 1$, is modeled as described above. Next, the connectivity of the network is defined by a sparse matrix and weights 1 are assigned to each line of unweighted network. The attacking mode proposed in this paper is applied to this IEEE 39 system and the lines with high betweenness values under different mode of attack are identified and classified as vulnerable. For each mode of attack 10 vulnerable lines are identified and every time each line is removed in the order of their betweenness index. In order to do the sensitivity analysis, first the efficiency of the network is calculated after each line attack. For IEEE 39 bus we have performed only line based attacking mode, node attacking mode will not give a good result due to less node in the network. From section $3 \cdot 1$ dynamic line betweenness attack, static line betweenness attack and high betweenness node less reactance line attack are done. Simulation result shows efficiency of the unweighted network drastically decreases under two attack mode one high betweenness dynamic line attack another attack is on high betweenness node with less reactance line attack in comparison to the random attack and high betweenness line static attack. In the figure $3 \cdot 3$, it can be clearly seen that the system is robust to random attacks where as fragile to intentional attack. After 10 such proposed attack the efficiency of the system decline to almost 29% and 35% whereas, the system is quite stable under random and high betweenness static attacks. Also the damage caused by different attack is quantified in terms of the relative size S of the largest connected

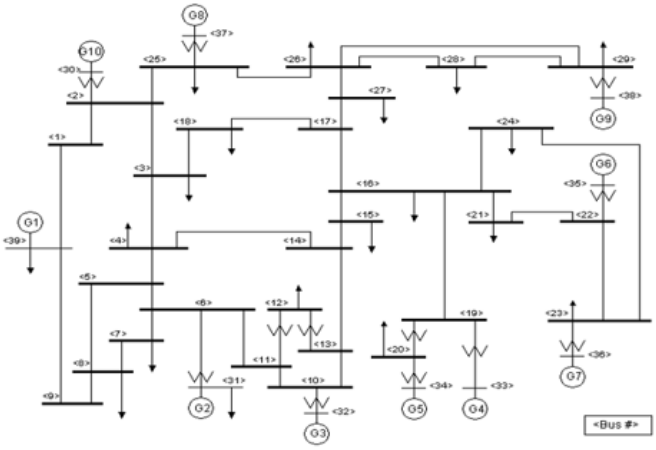

Figure 3.1: Schematic of a Power Network

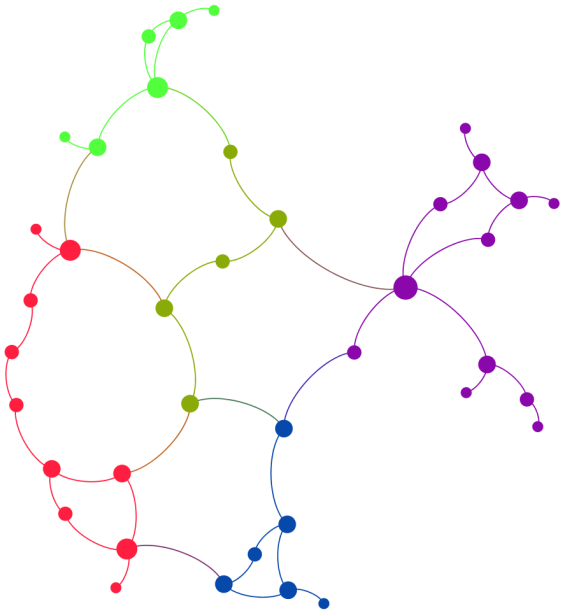

Figure 3.2: IEEE 39 modeled using gephi, degree distribution can be seen in terms of size of node

component. In the fig $3 \cdot 4$ we can see that the giant component size for dynamic line attack and high betweenness node less reactance line attack drops up to 20% to 28% in comparison to the random attack and static line attack. That means we are attacking most vulnerable lines in network.

3.3.2 IEEE 118 and 300 Bus System

Figure $3 \cdot 5$ shows the IEEE 118 bus system. The118 bus system is modeled in a similar way as described in IEEE 39 bus. After modeling simulation is run and the vulnerable lines identified similar to the IEEE 39 bus system

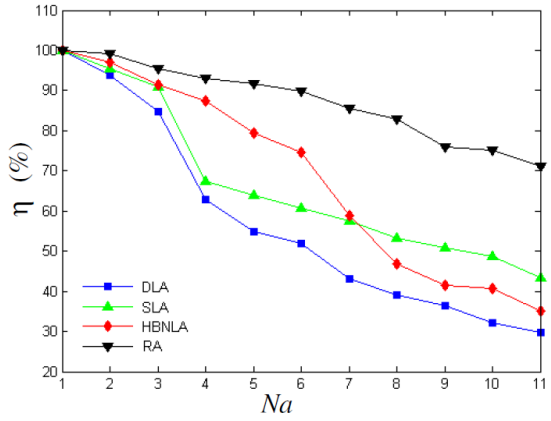

Figure 3.3: Effect of 4 mode of line attack on the efficiency of IEEE 39 bus system

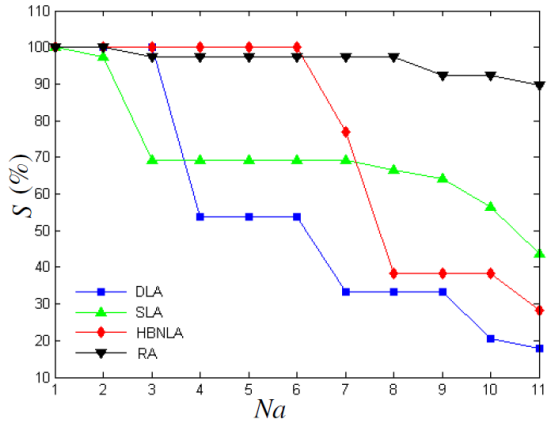

Figure 3.4: Drops in giant component size in IEEE 39 bus, result shown for 4 mode of line attacks

but only difference is that here vulnerable nodes also identified for different mode attack as described in section $3 \cdot 1$. As the small world network is quite robust to random attack, which already we have seen in IEEE 39 bus, hence we have not do any random attack for IEEE 118 and 300 bus. After each mode of attack 20 vulnerable line and nodes are identified and removed one by one to calculate efficiency and giant component of the network. In The figure $3 \cdot 7$ shows the effect of efficiency on IEEE 118 bus system after total 6 mode of attack (line and node attack). In three different mode of node attack the drop in efficiency is all most closer to each other, as we are not giving more emphasis on node attack, study says transmission lines are more vulnerable than node [42]. In the plot the attack on node shows drop is more for dynamic high degree node attack than other two mode of attack. In case of

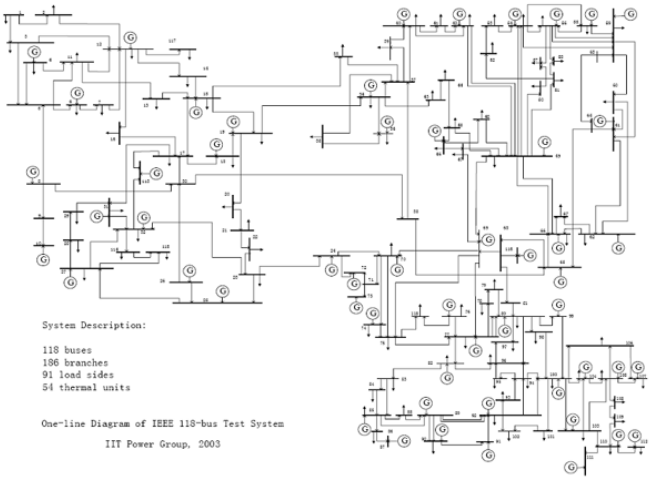

Figure 3.5: IEEE 118 Bus System

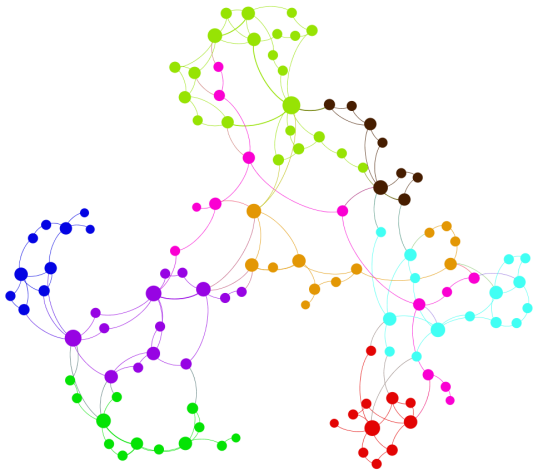

Figure 3.6: Topological structure of IEEE 118 bus system

line attack our proposed two mode of attack shows good result in comparison to static line attack, random attack is not performed here due to the robust ness of grid to this attack. In Figure $3 \cdot 8$ giant component size is calculated. The symbol star, square and upper triangle shows the line base attack result. Clearly we can see that for dynamic line attack and high betweenness node and less reactance line attack the giant component size drops nearly equal to 26% and 60% but in static line attack there is only a 3% of deviation in giant component size. In case of node attack due to dynamic high degree node the giant component size drops up to 25%. Basically if we analyze the results of IEEE 118 and IEEE 300 bus system, we can see that in case of both

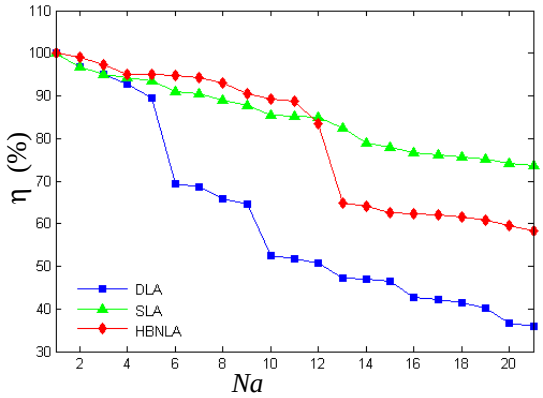

Figure 3.7: Effect of line attack on the efficiency of IEEE 118 bus system

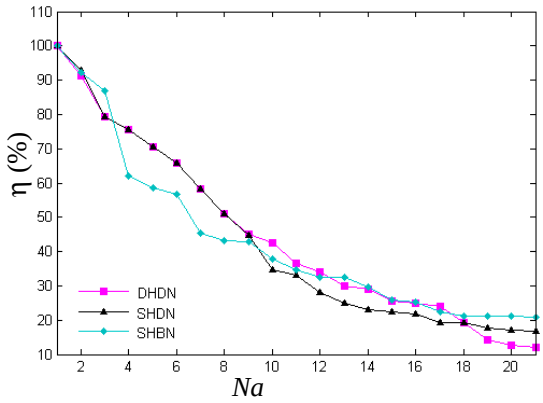

Figure 3.8: Effect of node attack on the efficiency of IEEE 118 bus system

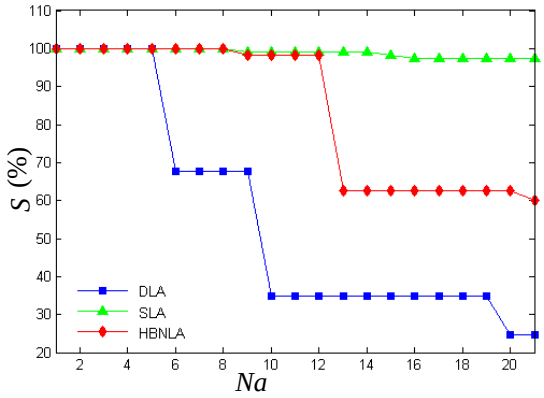

Figure 3.9: Drops in giant component size in IEEE 118 bus, result shown for line attacks

line and node attack, drops always more in dynamic type of attack. However our measure concern is line attack. The giant component size drops nearly about 22% after 20 line attack, which shows it is more vulnerable than other node. In case of IEEE 300, giant component drops completely to 0% after 20 attack. The efficiency drops to 30% and 40% for line attack and around

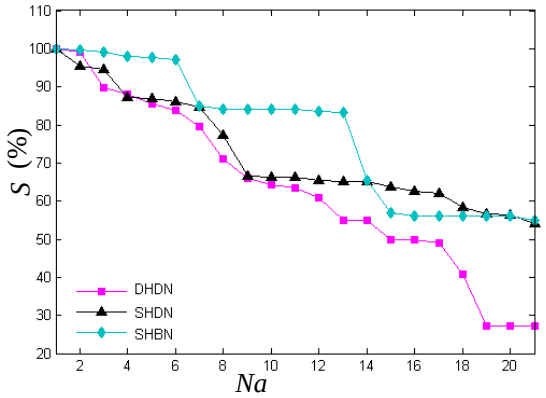

Figure 3.10: Drops in giant component size in IEEE 118 bus, result shown for node attacks

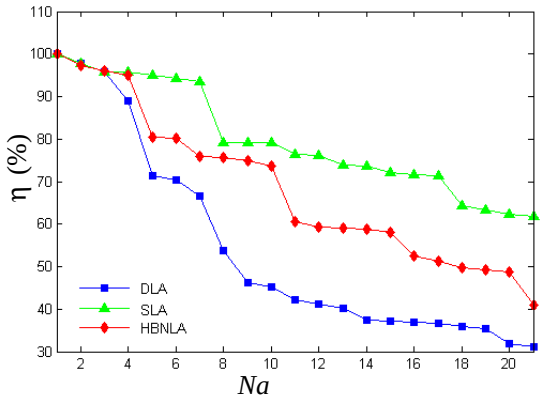

Figure 3.11: Effect of line attack on the efficiency of IEEE 300 bus system

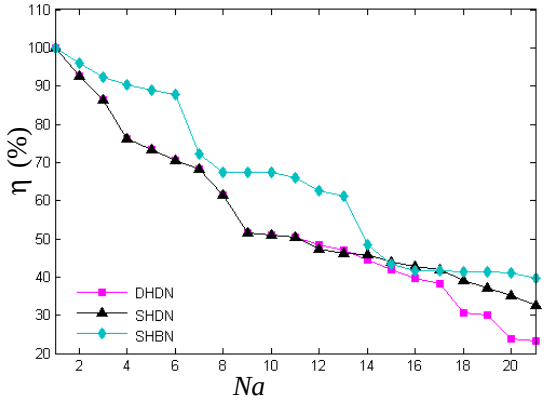

Figure 3.12: Effect of node attack on the efficiency of IEEE 300 bus system

25% for dynamic node attack. If we remove the line chosen by dynamic line attack, the giant component size and efficiency drops speedily and the grid will collapse completely after 20 attack. In figure $3 \cdot 9$ performance of IEEE 300 bus is measured. The network more fragile to proposed line attack.

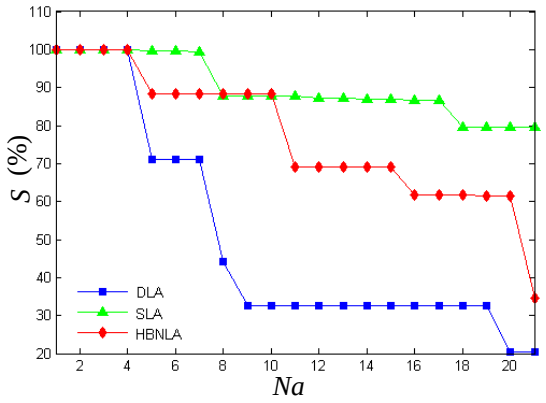

Figure 3.13: Drops in giant component size in IEEE 300 bus, result shown for line attacks

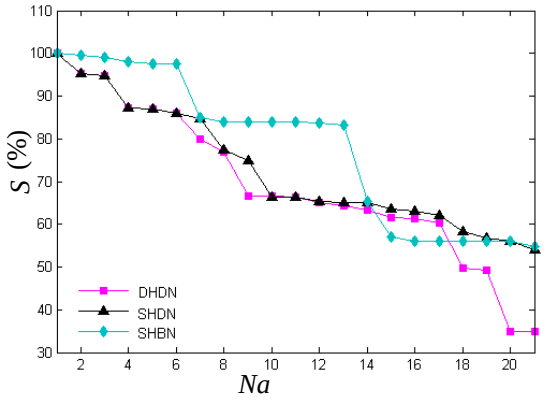

Figure 3.14: Drops in giant component size in IEEE 300 bus, result shown for node attacks

3.3.3 Discussion

It has been demonstrated that there are few links in every power network which can make it very vulnerable to attacks. It has been observed that in IEEE 39, the system is quite robust to random attacks and there is hardly any effect on the efficiency and giant component size of the network if the lines are randomly selected and removed. This was verified by 5 different sets of random attacks. Whereas, under targeted 3 different mode for line attack, the lines with high betweenness index are removed, the efficiency of the network drops sharply to almost 30% after 10 line attack and giant component size drop almost 20% and 30% for dynamic line and HBNLR attack. In IEEE 118 and 300 bus system also same result was found for 6 different type of attack, here only we have excluded random attack, in these two network node attack was also performed.

In our work we are dealing with relatively small size of networks with 39 118 and 300 nodes. Hence, increasing the number of attacks to 20 or 30 starts to deteriorate the performance of the network. Another big issue that, in these small network there are not many connection in between node are present and as we increase the number of attacks the chances of links with higher betweenness centrality index being removed increases. Also there are very less number of node present in our network, if we increase the node attack more than 10 than the system divided into many small part, for which we are not getting the required result. Further, in case of targeted attack, the drop in performance of network reduces as number of attacks is significantly increased. This is because with increased number of attacks, the identified links become less and less important. This is more prominent in the case of IEEE 39 bus system which has only 46 connections. Hence, we have considered only 10 attacks, which reflected good difference between random and targeted removals, throughout this study to validate our results but in IEEE 118 we have considered 20 attacks, for line attack the result is ok, but in case of node attack, after 10 attack it divided into several part, and the results deviate from original result. Overall, a more accurate study of this nature will further refine the results and point to the vulnerable nodes and transmission links. The shortest path betweenness approach is simple and efficient in identifying vulnerable connections in any network.

3.4 SUMMARY

This chapter has presented the structural vulnerability analysis of IEEE 39,118 and 300 bus power systems. Initially, the IEEE 39 bus has been analyzed based on betweenness centrality approach after that IEEE 118 and 300 bus has been analyzed based on node degree and centrality both for line and node. Some basic definition, parameters and algorithms relevant to this study have also been included in this chapter. Finally, two new vulnerable line identification index has been proposed based on the shortest path betweenness approach. The results have been verified by calculating the sen-

sitivity and giant component size of the network to random and targeted attacks.

Chapter 4

ANALYSIS OF WEIGHTED NETWORK

4.1 OVERVIEW

This chapter discusses the vulnerability assessment of a weighted network using betweenness centrality approach. Section $4 \cdot 2$ gives some preliminaries relevant to this study. Section $4 \cdot 3$ proposes the vulnerability analysis of IEEE 39, 188 and 300 bus power networks using the shortest path betweenness and node degree approach. This section explains the modelling of a power system so as to incorporate some of its electrical properties and also defines some of the network parameters and efficiency factors which are used in assessing the performance of the network. It also introduces the new betweenness index using the reactance of the transmission lines to weight the connection matrix and measure the vulnerability of a power network. Finally, the proposed methodology is demonstrated by a rigorous analysis on the IEEE 39 bus, IEEE 118 bus and IEEE 300 bus systems using the betweenness preferential edge and node removal.

4.2 PRELIMINARIES

On the very basic level, a real network can be modeled as a graph, consists of points termed as vertex or nodes which are connected to each other by some relationship. These connections or relationships are termed as edges. There are several parameters defined to measure the connectivity and intactness of

a network. The basic connectivity of a network can be defined by degree which is the number of edges or number of adjacent nodes connected to any node. Further, this information can be expanded over the network by degree distribution which gives the frequency of occurrence of each degree i.e. it represents the number of nodes in the network having a particular degree or in case of a growing network it is represented by a probability distribution and could be interpreted as chances of a node having a particular degree.

The biggest connected part of any network is termed as giant component and if there are any nodes left out due to failure or other reasons, they are said to form islands. Other measure like clustering coefficient defines the average closeness of a network. It represents the ease with which nodes can be reached from each other. It was assumed that in a small world network, the information is transmitted via the most efficient way that is the shortest number of steps which is termed as geodesic path in the network theory. In this chapter, we will use all this information is identifying the critical components (nodes and edges) and assessing the performance of the network.

4.3 ELECTRICAL MODEL OF A POWER NETWORK

In the previous chapter we studied, the unweighted undirected small world network. Analysis has been done over IEEE 39, 118 and 300 bus system. In this chapter we are interested to study the weighted small world network, and intention is to do the same attack done for unweighted network, and at last make a thorough analysis between weighted and unweighted network. Now our aim is to identify most vulnerable line and node based on the power flowing through any power network. In real power grid power flow is dependent on the transmission line parameters and node voltages. For simplification purpose we are using DC power flow model, where the line is considered to be lossless, which means the resistance is considered to be negligible. The power flow will then be dependent on the line reactance and node voltages. In such a case, the active power transmitted from node i to node j of the

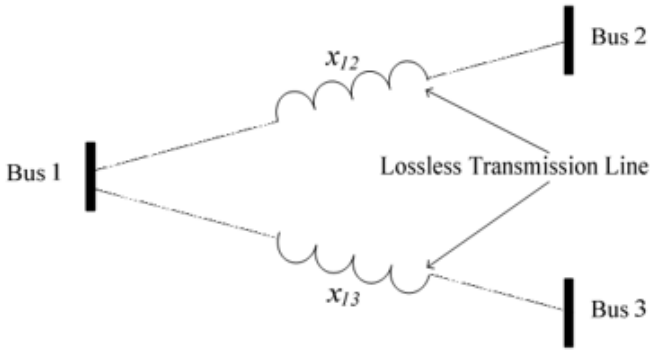

Figure 4.1: Simplified Power System Network

power network can be represented as following [25]:

$$P = \frac{v_i v_j}{x_{ij}} \sin \alpha_{ij} \tag{4.1}$$

Where P is the active power flowing through the line,v_i and v_j are the node voltage, α_{ij} is the phase angle between the voltages and x_{ij} is the reactance of the line. For simplicity we have ignored the node voltage and phase angle, now we can see from Equation $4 \cdot 1$ that the power flowing through transmission line is inversely proportional to the reactance of that line.

4.4 NEW BETWEENNESS INDEX

From equation $4 \cdot 1$, we can say that the amount of power flowing through any line of the transmission network is inversely proportional to its reactance. Thus, the reactance of a connecting line is considered as the weight in the connection adjacency matrix. Figure $4 \cdot 1$ shows a simple electrical model consist of 3 bus bar and 3 loss less transmission line, in which the resistance component is considered zero and only the reactance is taken into account. If the reactance of $x_{12} > x_{13}$, then more power will flow through the line from bus 1 to bus 3. So if there are many connection from highly loaded node, than definitely more power will flow through less reactive line giving it a higher priority in the analysis The number of times a line or node are used to transmit power throughout the power system is dependent on its position in the network and the value of its weight. According to motter and lai, the number of time shortest path passed through a node is considered as

load of that node, similarly we have assumed that number of shortest path passed through a line is the load over that line. This number is used as the betweenness index to identify the vulnerable lines of the power network. The lines with high betweenness index are classified as critical in order of their values. Thus, the reactance of a line together with its position helps to identify the vulnerable lines

4.5 PERFORMANCE OF A WEIGHTED POWER NETWORK

Until now, we have studied and analyzed the unweighted network with a concept that the shortest path is the most efficient way for transmitting any information through the network. In case of a unweighted network the shortest path is the minimum edges connected between two node but here we are discussing about a weighted network, which is completely different from a unweighted network. In our work we have considered reactance as the weight of each transmission line, now shortest path between two nodes is the minimum weighted path connected among all other path between them. As also mentioned in Chapter 2, shortest path can be used as a measure of efficiency for any network which can be defined as the inverse of characteristic path length [33]. In case of a weighted network more power will flow through a less reactive path or shortest path, which makes it important than other link. Thus the efficiency a link can be written as

$$w_{ij}=\frac{1}{x_{ij}} \qquad x_{ij} \quad is\ the\ reactance\ of\ the\ link \tag{4.2}$$

If two nodes are not connected, whether directly or indirectly, the distance between them will be infinite and the efficiency between them will be zero. The average efficiency of the whole network is [43]:

$$\eta=\frac{1}{N(N-1)}\sum_{i\neq j\in G} w_{ij} \tag{4.3}$$

or

$$\eta=\frac{1}{N(N-1)}\sum_{i\neq j\in G} \frac{1}{x_{ij}} \tag{4.4}$$

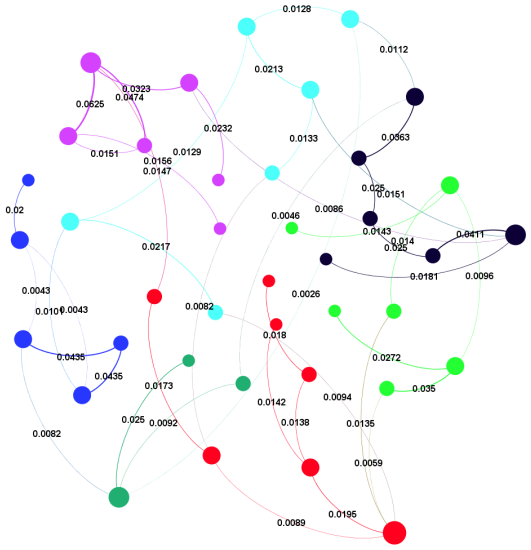

Figure 4.2: IEEE 39 weighted bus power system

Where G is the network, J is the efficiency of the network, i and j represent nodes, N is the no of node present in the network.

4.6 CASE STUDIES

The case of IEEE 39, 118 and 300 bus system are under taken and the techniques defined in previous sections are used to identify the vulnerable lines. The results are verified by the proposed attack strategies and verified by sensitivity and giant component size analysis.

4.6.1 IEEE 39 Bus System (Weighted)

Previously we have analyzed the unweighted IEEE 39 bus power system, after performing different attack strategies we have concluded that, highly vulnerable line can be identified by dynamic line attack and high degree node less reactance line attack. These attacks are now extended to words weighted network, we will analyze how the weighted small world network perform after these attack and the result will compare with unweighted network result. Once the vulnerable links of the network have been identified according to our different attack strategies, the system is attacked and sensitivity of the network as well as giant component size to these attacks is calculated. Firstly, the system is subject to random attacks and a total of 10 random links

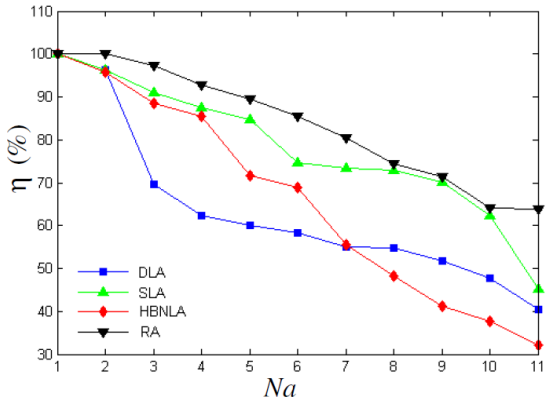

Figure 4.3: Drops in efficiency of IEEE 39 bus weighted network

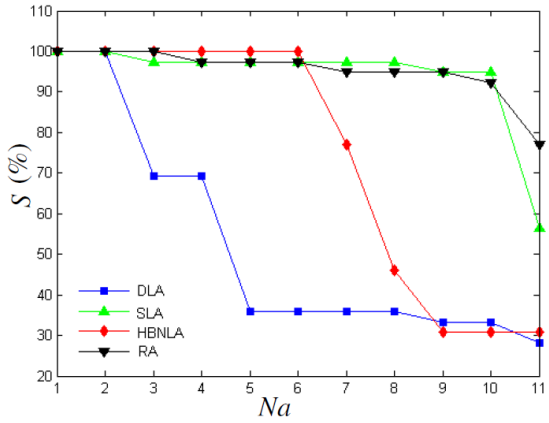

Figure 4.4: Drops in Giant component size of IEEE 39 bus weighted network

are removed one after another. A total of 5 different set of such attacks are conducted and the mean and standard deviation is calculated. This results are consistent and valid for most random attacks. Next, the system is subject to intentional attack and a total of 10 links identified as vulnerable are removed in the order of their betweenness index. Efficiency and giant component size after each attack is calculated. The figure $4 \cdot 3$ shows the drops in efficiency for random and intentional attack. After 10 attack the efficiency for random attack the network efficiency drops up to 65% whereas for our proposed attack the efficiency drop to 30% and 40%. Similarly in the figure $4 \cdot 4$ we can see that after only 2 attack giant component size for dynamic line attack speedily drops to 70% and after 10 attack it reaches to 30%, may be few more attack drop will reach to 0. But for random attack network is more robust which can be seen from figure $4 \cdot 3$ and $4 \cdot 4$ as well

as our proposed attack model gives good result than static attack method proposed in various paper.

4.6.2 IEEE 118 and 300 Bus System

The IEEE 118 bus weighted network is model same as IEEE 39 bus power system. The global efficiency J of a network was first introduced by Latora and Marchiori [13]. He proposed efficiency for both weighted and unweighted network, however in our work, we also analyzed that drops in efficiency after each line attack for weighted and unweighted network continue, even drop is more during dynamic line and high betweenness node and less reactance line attack also this strategies works well with giant component size. A sharp drop in giant component size can be seen in figure $4 \cdot 6$, and after 20 such attack drops decline to 35%, which is more than enough to destroy a network completely. In case of a node attack, static high betweenness node attack give more accurate result. For unweighted network dynamic high degree node attack is more vulnerable than any other attack but when we start working with weighted network, rather than dynamic node degree attack and static high betweenness node attack gives idea about most vulnerable node in these network. This time the size of the network is comparatively larger than 39 bus system so, there are more alternate paths for power flow. Hence, the effect of random attack on the performance of the system is even less. On the other hand, after 20 vulnerable links are removed, the network efficiency drops to almost 46% and the giant component size drops to 75% for the proposed attack in IEEE 300 weighted network. According to Albert et. al. heterogeneous a network is in terms of, e.g.,degree distribution, the more robust it is to random failures, while, at the same time, it appears more vulnerable to deliberate attacks on highly connected nodes. But weighted network does not showing the behavior of a heterogeneous network.

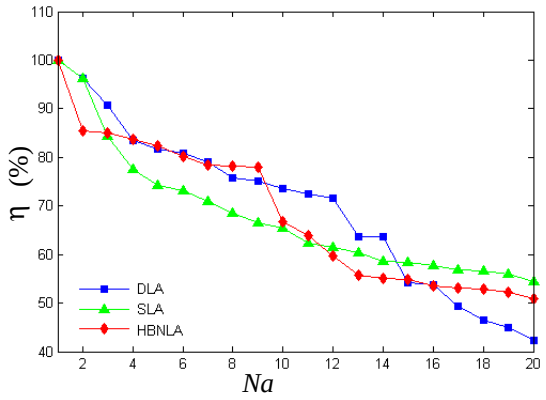

Figure 4.5: Drops in efficiency of IEEE 118 bus weighted network line attack

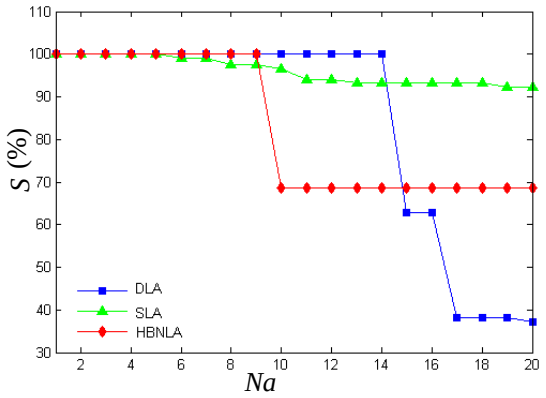

Figure 4.6: Drops in Giant component size of IEEE 118 bus weighted network line attack

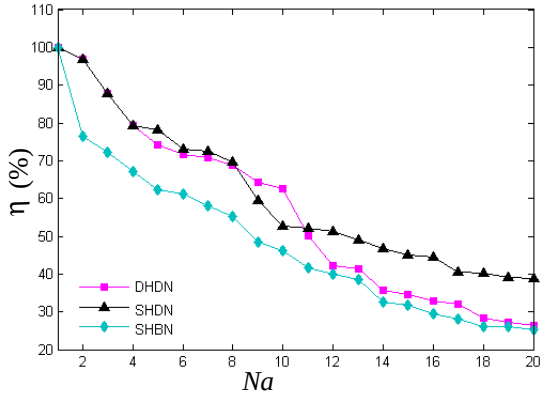

Figure 4.7: Drops in efficiency of IEEE 118 bus weighted network node attack

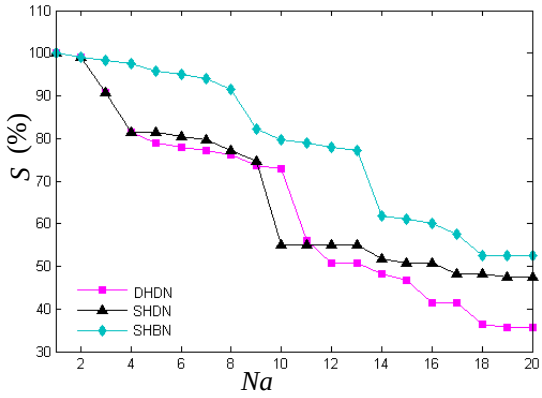

Figure 4.8: Drops in Giant component size of IEEE 118 bus weighted network node attack

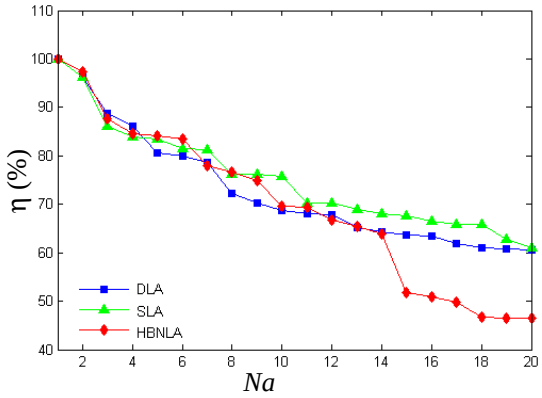

Figure 4.9: Drops in efficiency of IEEE 300 bus weighted network line attack

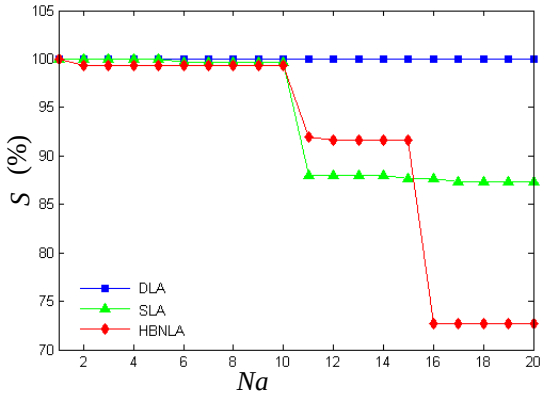

Figure 4.10: Drops in Giant component size of IEEE 300 bus weighted network line attack

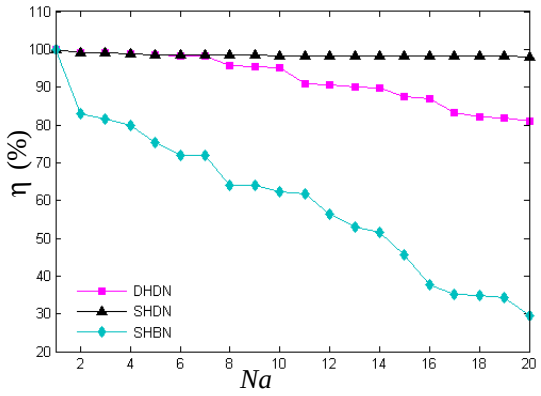

Figure 4.11: Drops in efficiency of IEEE 300 bus weighted network node attack

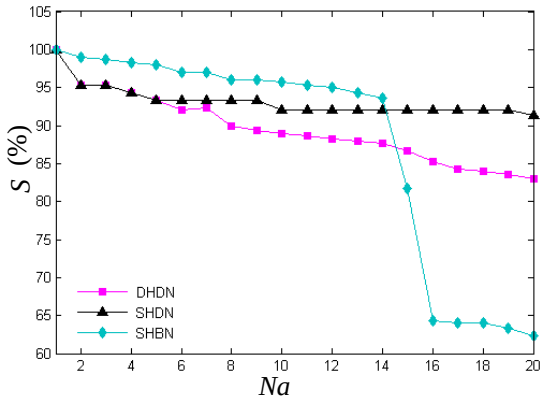

Figure 4.12: Drops in Giant component size of IEEE 300 bus weighted network node attack

4.6.3 Discussion

There are few links in every power network which can make it very vulnerable to intentional attacks. It has been observed in IEEE 39 bus, that the system is quite robust to random attacks and there is hardly any effect on the efficiency and giant component size of the network if the lines are randomly selected and removed. This was verified by 6 different sets of random attacks in each case. Whereas, under intentional attack, where the lines with high betweenness index under different mode of attack are removed, the efficiency and giant component size of the network drops sharply to almost 30% and 35% for unweighted network and 30% and 40% for weighted network after 10 attacks in the IEEE 39 bus system and in IEEE 118 and 300 bus system significant drops can seen after 20 attacks from the given figure. We are dealing with relatively small size of networks with 39, 118 and 300 nodes Hence, in-

creasing the number of attacks to 20 starts to deteriorate the performance of the network even with random attack, because there are very few connections and as we increase the number of attacks the chances of links with higher centrality index being removed increases. Further, in case of intentional attack, the drop in performance and giant component size of a network reduces as number of attacks is significantly increased. This is because with increased number of attacks, the identified links become less and less important. This is more prominent in the case of IEEE 39 bus system which has only 46 connections. Hence, we have considered only 10 attacks, which reflected good difference between random and intentional attack both in weighted and unweighted network. Another new thing we analyzed that, the IEEE aa8 and 300 weighted network are not affected much more for dynamic high degree node attack.

4.7 SUMMARY

This chapter has presented the structural vulnerability analysis of weighted and unweighted power systems. Initially, the IEEE 39 bus has been analyzed. Further, few techniques have been described to model a weighted power system as a network .Some basic definition, parameters and algorithms relevant to this study have also been included in this chapter. Finally, a new concept is added here to get highly vulnerable betweenness index has been proposed based on the shortest path betweenness approach. The new betweenness index identifies the vulnerable lines based on shortest path concept. The results have been verified by calculating the sensitivity and giant component size of the network to random and targeted attacks.

Chapter 5

CONCLUSIONS AND FUTURE RESEARCH

5.1 OVERVIEW

This chapter summarizes the complete work done in this research and gives an overall picture of the work and results achieved. Section 5.2 gives an overall conclusion and outlines the results of this thesis. Finally, Section 5.3 concludes with future research scope.

5.2 CONCLUSIONS

After thorough analysis this thesis has demonstrated that, in every power system, there are a few lines as well as nodes are present, which are responsible for cascading failure. If those lines or nodes fail or are intentionally attacked then the performance of the system drops considerably where as other less important component do not have much impact on its performance. It has also been shown that if the critical lines and nodes fail then power redistributed to the adjacent lines, which creates a over load condition might force it to fail, causing further load shift and failure. If this process continue than this could eventually lead to cascading failure and serious blackouts.

The cascading failures have been further assessed and analyzed using network theory, in which attempts have been made to predict the group of lines

which could be affected in case of any outages and the sequence in which they might fail. This also helps to predict the critical lines and the depth to which any failure may penetrate in case of cascades. Overall, it can be concluded that, it is important to identify such vulnerable elements to be able to focus more resources on them and monitor them to enhance system security and reliability.

The major results and contribution of this research can be summarized as below

- A new betweenness index has been proposed based on the latest developments in the complex network theory.
- This new index can identify the vulnerable lines based on their position in the network and behaviour of grid after attack.
- The results are verified by calculating sensitivity and giant components of the network to random as well as targeted attack.
- System is more vulnerable to proposed attack, than random, and static betweenness attack.
- Since the links and nodes in any power network make it vulnerable to some mode of attack, it is therefore important to identify these links and node, whose maintenance can increase the reliability of the networks.

5.3 FUTURE RESEARCH SCOPE

Finally, a few future research directions are listed below before concluding this thesis:

- Pure topological metrics could give a misleading result [7], which may be far from real physical behaviors of power grids. More realistic models are therefore necessary which can incorporate real electrical features of a power grid (like, electrical distance, PTDF and LODF).

- Topological analysis can also be extended to analyse a power distribution network to identify the critical distribution of lines after one attack.

5.4 SUMMARY

In summary, a power system is very dynamic in nature and extremely complicated, so it is difficult to consider all the electrical and topological properties at the same time. AC analysis of power system is very complex, even real time application is also not possible. However, this thesis gives a new direction to the use of CNT in power system research, which will improve structural vulnerability assessment and identification of important lines and nodes. The overall goal of applying the Complex Network Theory in solving a few problems of vulnerability analysis and fault location in power systems has been achieved.

Bibliography

[1] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, "Network flows: theory, algorithms, and applications," 1993.

[2] T. G. Lewis, *Network science: Theory and applications*. Wiley, 2011.

[3] S. H. Strogatz, "Exploring complex networks," *Nature*, vol. 410, no. 6825, pp. 268–276, 2001.

[4] M. Ding and P. Han, "Reliability assessment to large-scale power grid based on small-world topological model," in *Power System Technology, 2006. PowerCon 2006. International Conference on*. IEEE, 2006, pp. 1–5.

[5] P. Hines and S. Blumsack, "A centrality measure for electrical networks," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008, pp. 185–185.

[6] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the italian electric power grid," *Physica A: Statistical Mechanics and its Applications*, vol. 338, no. 1, pp. 92–97, 2004.

[7] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-worldnetworks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[8] S. Milgram, "The small world problem," *Psychology today*, vol. 2, no. 1, pp. 60–67, 1967.

[9] L. d. F. Costa, F. A. Rodrigues, G. Travieso, and P. Villas Boas, "Characterization of complex networks: A survey of measurements," *Advances in Physics*, vol. 56, no. 1, pp. 167–242, 2007.

[10] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics reports*, vol. 424, no. 4, pp. 175–308, 2006.

[11] M. E. Newman, "The structure and function of complex networks," *SIAM review*, vol. 45, no. 2, pp. 167–256, 2003.

[12] P. Erd6s and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hungar. Acad. Sci*, vol. 5, pp. 17–61, 1960.

[13] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical review letters*, vol. 87, no. 19, p. 198701, 2001.

[14] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[15] D. J. Watts, *Small worlds: the dynamics of networks between order and randomness.* Princeton university press, 1999.

[16] M. Mitchell, "Complex systems: Network thinking," *Artificial Intelligence*, vol. 170, no. 18, pp. 1194–1212, 2006.

[17] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[18] A. H. Dekker and B. D. Colbert, "Network robustness and graph topology," in *Proceedings of the 27th Australasian conference on Computer science-Volume 26.* Australian Computer Society, Inc., 2004, pp. 359–368.

[19] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of scale-free networks: error and attack tolerance," *Physica A: Statistical Mechanics and its Applications*, vol. 320, pp. 622–642, 2003.

[20] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, p. 056109, 2002.

[21] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

[22] V. Gol'dshtein, G. Koganov, and G. Surdutovich, "Vulnerability and hierarchy of complex networks," *arXiv preprint cond-mat/0409298*, 2004.

[23] M. Di Santo, A. Vaccaro, D. Villacci, and E. Zimeo, "A distributed architecture for online power systems security analysis," *Industrial Electronics, IEEE Transactions on*, vol. 51, no. 6, pp. 1238–1248, 2004.

[24] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control.* Wiley-Interscience, 2012.

[25] L. Zongxiang, M. Zhongwei, and Z. Shuangxi, "Cascading failure analysis of bulk power system using small-world network model," in *Probabilistic Methods Applied to Power Systems, 2004 International Conference on.* IEEE, 2004, pp. 635–640.

[26] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Physical Review E*, vol. 69, no. 2, p. 025103, 2004.

[27] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, p. 045104, 2004.

[28] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the european power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2465–2475, 2007.

[29] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the european power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, p. 026102, 2008.

[30] S. Mei, *Power grid complexity.* Tsinghua University Press, 2011.

[31] D. L. Pepyne, "Topology and cascading line outages in power grids," *Journal of Systems Science and Systems Engineering*, vol. 16, no. 2, pp. 202–221, 2007.

[32] K. Sun, "Complex networks theory: A new method of research in power grid," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES.* IEEE, 2005, pp. 1–6.

[33] V. Latora and M. Marchiori, "Economic small-world behavior in weighted networks," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 32, no. 2, pp. 249–263, 2003.